REMARKS

REJECTIONS UNDER 35 U.S.C. § 102(e)

In paragraph 4 of the present office action, claims 1-23 have been rejected under 35 U.S.C. § 102(e) as being anticipated by *Atkinson et al.* (U.S. Patent No. 5,892,904 - *"Atkinson"*). These rejections are respectfully traversed, and favorable reconsideration of the claims is hereby requested.

Atkinson relates to data encryption, and specifically teaches a method of creating an electronic signature using a public/private key pair. The electronic signature ensures the authenticity of the document being sent, analogously to a written signature. Various methodologies are known in the art for creating a digital signature. In the passages cited by the Examiner in *Atkinson*, this digital signature is created using a private key known only to the sender and a public key available to anyone. The public key is typically part of a digital certificate issued by a certification authority (CA) or agency. Thus, the sender "signs" a document using his private key, which encrypts the signature. To decrypt the signature, the receiver of the document uses the sender's public key. *Atkinson* teaches a second layer of security by requiring the receiver to use a second public key (provided by the CA) to decrypt the sender's public key. (*Atkinson* col. 3, lines 13-40; col 6, line 34 to col. 8, line 29.)

The present invention does not claim the use of data encryption and/or digital signatures as taught by *Atkinson*. Likewise, *Atkinson* does not teach or suggest a method of identifying suspected copyright infringing material as taught by the present invention.

The present invention describes a method and system for identifying suspected copyright infringing material by:

- "receiving a selectable data stream of suspected copyright infringing material"
- "generating a first electronic signature" of the suspected copyright infringing material and a "second electronic signature for an original copyright material", wherein each

electronic signature is a "distillation," and

- comparing the two electronic signatures, wherein a match of the signatures indicates a likelihood that the two materials are the same.

To illustrate, consider a paragraph of text from a webpage that is suspected of containing material that is so similar to other text being used that there may be a copyright infringement. The suspected copyright infringing material may be located using key data for identifying passages of text, such as used by a search engine to locate key terms on websites on the Internet. The suspected copyright infringing material is downloaded in a stream (orderly stream of data), which is then used to generate "a first electronic signature." In a preferred embodiment, this "first electronic signature" is generated through the use of a linear feedback shift register, as depicted in Figure 5 and described in the present specification. The stream of data is converted into a binary data stream (converted from a stream of bytes to a stream of bits), and run through the depicted shift register. The shift register uses a combination of latches and logic gates (depicted as OR gates) to create a unique 16-bit "first electronic signature" for the block of data. That is, after running the entire binary stream through the linear feedback shift register, the register will contain a non-exclusive 16-bit value that can (likely) only be generated by the binary stream resulting from a unique block of data, such as a paragraph of text. Note that the non-exclusive nature of the electronic signature is that different blocks of data may generate the same electronic signature, due to the inherent nature of distilling the data to a smaller data form than the original data. This electronic signature is then compared with a second electronic signature for a block of data (original copyright material) owned/used by the user of the present invention. If the two signatures match, then the two texts are possibly identical, indicating a copyright infringement. In a preferred embodiment, the two blocks of data (the suspected copyright infringing material that was downloaded and the user's own original copyright material) are then visually compared.

Alternatively, the paragraph or other defined block of text can be parsed into smaller pieces (data segments), and each smaller data segment is evaluated as above. This allows the user to identify similar or identical passages of text. If similar or identical passages are identified, in a

preferred embodiment the two passages are then displayed on-screen for a visual examination by the user. Thus, the user is able to ensure that a copyright infringement is not committed, either inadvertently (by the user) or intentionally (by another party), on all or part of a passage.

It is axiomatic that for anticipation under 35 U.S.C. § 102 the reference must teach every aspect of the claimed invention. *MPEP § 706.02.*

Regarding **Claim 1,** the cited prior art does not teach receiving streamed data segments of suspected copyright infringing material, generating an electronic signature for the data segments, and comparing the signature of the suspected material to an electronic signature of original copyright material wherein a match of said data segment signature with said original copyright material signature indicates that said data segment and said original copyright material are likely the same. The electronic signature is a distillation generated according to the data segment (or original copyright material) itself, and is not a "digital signature" as described by *Atkinson* to authenticate a transmission. The distillation cannot be used to reconstruct the data segment (original copyright material). That is, the electronic signature of the present invention is a unique abbreviated value generated by logic, such as a shift register, to generate a unique value that identifies the data segment. The data segment provides the data required to generate the specific value (electronic signature), but the specific value, being a distillation, is incapable of reconstructing the data segment. Thus, the present invention is not an encryption/decryption method and system as described by *Atkinson.*

Likewise, *Atkinson* does not teach the feature of comparing electronic signatures for different data (original copyright material and suspected copyright infringing material), wherein a match of the signatures indicates that the materials are the same. *Atkinson's* "digital signal" is a single data that is decrypted by a receiver to authenticate the identity of the sender.

Claim 2 further describes the process of evaluating data that is on the Internet, and converting it into a stream for processing as described above.

As the prior art does not teach all of the features of claims 1 and 2, Applicants respectfully request that the Examiner withdraw the rejections of claims 1 and 2.

Regarding **Claim 5**, the present invention claims the additional feature of "visually examining" the "suspected copyright infringing material" if the first and second signatures match. That is, when a suspected copyright infringing material is identified, it is displayed on-screen to the user, who then compares the suspected copyright infringing material with the user's own original copyright material. *Atkinson* does not teach or suggest such a visual comparison of data segments. As the prior art does not teach all of the features of claim 5, Applicants respectfully request that the Examiner withdraw the rejection of claim 5.

Regarding **Claim 3**, the present invention claims the additional features of "parsing said streamed data of suspected copyright infringing material into...data segments" and "generating a...signature for each...data segment." As described above in the description of the present invention, this allows the user to identify smaller passages of text that are identical to the original copyright material, even though the entire block of text may not be identical. *Atkinson* does not teach parsing a streamed data. Rather, *Atkinson* only teaches providing a separate digital signature for an entire file being transmitted. **Claim 4** teaches a similar feature for the original copyright material to afford the ability to compare signatures of the two parsed data segments, as claimed in **Claim 6**. As the prior art does not teach all of the features of claims 3, 4 and 6, Applicants respectfully request that the Examiner withdraw the rejection of claims 3, 4 and 6.

Claims 7 - 12 are system claims including features described above for claims 1 - 6. Similarly, **Claims 18 - 23** are computer program claims including features described for claims 1 - 6. Therefore the arguments for claims 1 - 6 presented above are hereby made for claims 7 - 20 and 23. As the prior art does not teach the features of claims 7 - 12 and 18 - 23, Applicants respectfully request that the Examiner withdraw the rejection fo claims 7 - 20 and 23.

Regarding new **Claims 24 - 25**, the additional feature of using a feedback shift register, as

described above in a preferred embodiment of the present invention, is claimed. *Atkinson* neither teaches nor suggests such a feature, and therefore Applicants respectfully request allowance of claims 24 - 25.

Regarding new **Claim 26**, means for "storing a first electronic signature for an original copyright material" as described above is specifically claimed. As *Atkinson* neither teaches nor suggests such a feature, and therefore Applicants respectfully request allowance of claim 26.

Regarding new **Claims 27 - 28**, the additional features of visually examining suspected copyright infringing material is performed with a predetermined number of signature matches is exceeded. *Atkinson* neither teaches nor suggests such features, and therefore Applicants respectfully request allowance of claims 27 - 28.

CONCLUSION

For the reasons stated, Applicants now respectfully request a Notice of Allowance for all pending claims.

No extension of time is believed to be required for responding to the current office action. However, in the event an extension of time is required, please consider that extension requested and please charge the fee for that extension, as well as any other fee necessary to further the prosecution of this application to **IBM Corporation Deposit Account No. 09-0447**.

Respectfully submitted,

James E. Boice
Registration No. 44,545
BRACEWELL & PATTERSON, L.L.P.
P.O. Box 969
Austin, Texas 78767-0969
(512) 343-6116

ATTORNEY FOR APPLICANTS

VERSION WITH MARKINGS TO SHOW CHANGES

IN THE CLAIMS

Please **amend** claims 1-12 and 18-23, **add** claims 24 - 28 and **cancel** claims 13-17 as indicated.

1. (Amended) A method for detecting copyright violation, said method comprising [the following steps]:

receiving [streamed] a selectable data [segments] stream of suspected copyright infringing material;

generating [an] a first electronic signature for [each] said data [segment] stream of said suspected copyright infringing material, said first electronic signature being a distillation, of said data stream, that is incapable of reconstructing said data stream by direct decipherment;

generating a second electronic signature for an original copyright material, said second electronic signature being a distillation, of said original copyright material, that is incapable of reconstructing said original copyright material by direct decipherment; and

comparing [each said signature for each said data segment of said suspected material to electronic signatures of original copyright material] said first electronic signature with said second electronic signature, wherein a match of said first electronic signature with said second electronic signature indicates a likelihood that said suspected copyright infringing material and said original copyright material are the same.

2. (Amended) The method of Claim 1, further comprising:

[extracting streamed data from the Web onto a server connected to the Internet; and

converting said streamed data to a binary stream] receiving said data stream of suspected copyright infringing material from the Internet.

3. (Amended) The method of Claim [2] 1, further comprising:

parsing said [streamed] data stream of suspected copyright infringing material into suspected

copyright infringing material data segments; and

generating a suspected copyright infringing material data segment electronic signature for each said [streamed] suspected copyright infringing material data segment, each said suspected copyright infringing material data segment electronic signature being a distillation of a corresponding said suspected copyright infringing material data segment.

4. (Amended) The method of Claim [1] 3, further comprising:

parsing said original copyright material into original copyright material data segments; and

generating an original copyright material data segment electronic signature for each said original copyright material data segment, each said original copyright material data segment electronic signature being a distillation of a corresponding said original copyright material data segment.

5. (Amended) The method of Claim 1, further comprising:

[performing signature analysis on said streamed data segments; and]

determining that said first electronic signature and said second electronic signature are a match; and

visually examining said [data segments] suspected copyright infringing material having said first electronic signature matching said second electronic signature of [matching any] said original copyright data [segments] material.

6. (Amended) The method of Claim [1] 4, further comprising:

[providing key data critical to recognizing said copyright material for searching the Internet for infringing copyright material] determining that at least one of said suspected copyright infringing material data segment electronic signatures matches at least one of said original copyright material data segment electronic signatures; and

visually examining said suspected copyright infringing material data segment having said suspected copyright infringing material data segment electronic signature matching said original copyright material data segment electronic signature.

7. (Amended) A system for detecting copyright violation, said system comprising:

receiving means for receiving [streamed] a selectable data stream of suspected copyright infringing material;

signature generation means for generating a first electronic [signatures] of said suspected material and a second electronic signature of an original copyright material, each said electronic signature being a distillation of material incapable of reconstructing said suspected material or said original copyright material by direct decipherment; and

comparator means for comparing [each] said first electronic signature with said second electronic signature, [for each said data segment of said suspected material to electronic signatures of original copyright material] wherein a match of said first electronic signature with said second electronic signature indicates a likelihood that said suspected copyright infringing material and said original copyright material are the same.

8. (Amended) The system of Claim 7, further comprising:

[extraction means for extracting streamed data from the Internet onto a server connected to the Internet; and

binary conversion means for converting said streamed data to a binary stream] means for receiving said data stream of suspected copyright infringing material from the Internet.

9. (Amended) The system of Claim [8] 7, further comprising:

parsing means for parsing said [streamed] data stream of suspected copyright infringing material into suspected copyright infringing material data segments; and

means for generating a suspected copyright infringing material data segment electronic signature for each said [streamed] suspected copyright infringing material data segment, each said suspected copyright infringing material data segment electronic signature being a distillation of a corresponding said suspected copyright infringing material data segment.

10. (Amended) The system of Claim [7] 9, further comprising:

parsing means for parsing said original copyright material into original copyright material

data segments; and

means for generating an original copyright material data segment electronic signature for each said original copyright material data segment, each said original copyright material data segment electronic signature being a distillation of a corresponding said original copyright material data segment.

11. (Amended) The system of Claim 7, further comprising:

[comparison means for performing signature analysis on said streamed data segments; and]

means for determining that said first electronic signature and said second electronic signature are a match; and

means for visually displaying [and examining] said suspected copyright infringing material having said first electronic signature matching said second electronic signature of said original copyright material. [data segments matching any said copyright data segments if matching signatures exceed a predetermined number.]

12. (Amended) The system of Claim [7] 10, further comprising:

[key data critical to recognizing said copyright material for searching the Internet for infringing copyright material.]means for determining that at least one of said suspected copyright infringing material data segment electronic signatures matches at least one of said original copyright material data segment electronic signatures; and

means for visually examining said suspected copyright infringing material data segment having said suspected copyright infringing material data segment electronic signature matching said original copyright material data segment electronic signature.

13. (Cancelled) [A system for detecting copyright violation, comprising:

a server connected to the Internet for storing copyright material;

a search engine available to said server for searching the Internet;

receiving means on said server for receiving streamed data of suspected copyright infringing material;

signature generation means for generating electronic signatures of said suspected material; and

comparator means for comparing each said signature for each said data segment of said suspected material to electronic signatures of original copyright material.]

14. (Cancelled) [The system of Claim 13, further comprising:

means for loading said copyright material onto said server for comparison to infringing copyright material.]

15. (Cancelled) [The system of Claim 13, further comprising:

data critical to said copyright material for searching the Internet for infringing copyright material.]

16. (Cancelled) [The system of Claim 13, further comprising:

data streaming means for streaming suspected infringing data files from locations on the Internet.]

17. (Cancelled) [The system of Claim 13, further comprising:

conversion means for converting said streaming data to a binary stream.]

18. (Amended) A computer program product within a computer readable medium having instructions for detecting copyright violation, said computer program product comprising:

instructions within said computer readable medium for receiving a selectable [streamed] data stream of suspected copyright infringing material;

instructions within said computer readable medium for generating [electronic signatures of said suspected material] a first electronic signature for said data stream of said suspected copyright infringing material, said first electronic signature being a distillation, of said data stream, that is incapable of reconstructing said suspected copyright infringing material by direct decipherment;

instructions within said computer readable medium for generating a second electronic

signature for an original copyright material, said second electronic signature being a distillation, of said original copyright material, that is incapable of reconstructing said original copyright material by direct decipherment; and

instructions within said computer readable medium for comparing [each said signature for each said data segment of said suspected material to electronic signatures of original copyright material] said first electronic signature with said second electronic signature, wherein a match of said first electronic signature with said second electronic signature indicates a likelihood that said suspected copyright infringing material and said original copyright material are the same.

19. (Amended) The computer program product of Claim 18, further comprising:

instructions within said computer readable medium for [extracting streamed data from the Web onto a server connected to the Internet; and

instructions within said computer readable medium for converting said streamed data to a binary stream] receiving said data stream of suspected copyright infringing material from the Internet.

20. (Amended) The computer program product of Claim [19] 18, further comprising:

instructions within said computer readable medium for parsing said [streamed] data stream of suspected copyright infringing material into suspected copyright infringing material data segments; and

instructions within said computer readable medium for generating a suspected copyright infringing material data segment electronic signature for each said [streamed] suspected copyright infringing material data segment, each said suspected copyright infringing material data segment electronic signature being a distillation of a corresponding said suspected copyright infringing material data segment.

21. (Amended) The computer program product of Claim [18] 20, further comprising:

instructions within said computer readable medium for parsing said original copyright material into original copyright material data segments; and

instructions within said computer readable medium for generating an original copyright material data segment electronic signature for each said original copyright material data segment, each said original copyright material data segment electronic signature being a distillation of a corresponding said original copyright material data segment.

22. (Amended) The computer program product of Claim 18, further comprising:

instructions within said computer readable medium for [performing signature analysis on said streamed data segments] determining that said first electronic signature and said second electronic signature are a match, thus enabling a visual examination of said suspected copyright infringing material.[; and

instructions within said computer readable medium for visually examining said data segments matching any said copyright data segments.]

23. (Amended) The computer program product of Claim [18] 21, further comprising:

instructions within said computer readable medium for [providing key data critical to recognizing said copyright material for searching the Internet for infringing copyright material.] determining that at least one of said suspected copyright infringing material data segment electronic signature matches at least one of said original copyright material data segment electronic signature.

24. (New) The method of Claim 1, further comprising:

generating said first electronic signature of said suspected copyright infringing material using a feedback shift register.

25. (New) The system of claim 7, further comprising:

a shift register for generating said electronic signature for each said data segment of said suspected material.

26. (New) A system for detecting a copyright violation, said system comprising:

means for storing a first electronic signature for an original copyright material, said first electronic signature being a distillation of said original copyright material;

means for identifying a suspected copyright infringing material that is suspected of being the same as said original copyright material;

means for generating a second electronic signature for said suspected copyright infringing material, said second electronic signature being a distillation, of said data stream, that is incapable of reconstructing said data stream by direct decipherment; and

means for comparing said first electronic signature with said second electronic signature, wherein a match of said first electronic signature and said second electronic signature indicates a likelihood that said original copyright material and said suspected copyright infringing material are the same, thus indicating a copyright violation.

27. (New) The method of claim 5, wherein said visual examination is performed upon said matches of said signatures exceeding a predetermined number of occurrences.

28. (New) The system of claim 12, wherein said visual examination is performed upon said matches of said signatures exceeding a predetermined number of occurrences.